**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of the Claims:**

Claims 1-27 (Cancelled)

28. (New) A method of managing access to a network, comprising the steps of:

providing a challenge-handshake protocol within an Extensible Authentication Protocol for authentication between a client and the network; and

deriving a network session key and a client session key, whereafter successful authentication of both the client to the network and the network to the client, the network session key is used to both create a packet signature and to encrypt a key value of a multicast key that is transmitted from the network to the client.

29. (New): The method of claim 28, wherein the challenge-handshake protocol in the step of providing is a CHAP (Challenge-Handshake Authentication Protocol).

30. (New): The method of claim 28, wherein authentication in the step of providing is performed mutually between the client and the network.

31. (New): The method of claim 28, wherein the challenge-handshake protocol comprises the step of mutually authenticating a client and the network in response to a single sign-on by a user of the client.

32. (New): The method of claim 28, wherein the challenge-handshake protocol in the step of providing facilitates authentication between the network and the client, which client is a wireless client.

33. (New): The method of claim 28, wherein the challenge-handshake protocol in the step of providing facilitates authentication between the network and the client, which client is a wired client.

34. (New): The method of claim 28, wherein the client session key is derived independently of the network session key, which both the network session key and the client session key are utilized for enabling secure communications between the client and the network.

35. (New): The method of claim 34, wherein the network session key is derived from a username of a user input to the client and transmitted to the network.

36. (New): The method of claim 28, wherein the challenge-handshake protocol in the step of providing is utilized between an authentication server disposed on the network and the client, the authentication server performing an authentication of the client, followed by the client performing an authentication of the network.

37. (New): The method of claim 28, wherein the network includes an authentication server disposed thereon for providing authentication services and a network access server disposed thereon for providing communications between the client and the authentication server, whereafter successful mutual authentication between the authentication server and the client, the authentication server passes a session key to the network access server utilizing vendor-specific attribute data.

38. (New): The method of claim 28, wherein the client is a wireless client including a network interface device, the network interface device adapted to host the challenge-handshake protocol utilized for authentication between the wireless client and the network.

39. (New): A method of managing access to a network, comprising the steps of:

providing a challenge-handshake protocol within an Extensible Authentication Protocol for authentication between a client and the network;

wherein the network includes an authentication server disposed thereon for providing authentication services and a network access server disposed thereon for providing communications between the client and the authentication server, whereafter successful mutual authentication between the authentication server and the client, the authentication server passes a session key to the network access server utilizing vendor-specific attribute data.

40. (New): The method of claim 39, wherein the challenge-handshake protocol in the step of providing is a CHAP (Challenge-Handshake Authentication Protocol).

41. (New): The method of claim 39, wherein the challenge-handshake protocol comprises the step of mutually authenticating a client and the network in response to a single sign-on by a user of the client.

42. (New): The method of claim 39, wherein the challenge-handshake protocol in the step of providing facilitates authentication between the network and the client, which client is a wireless client.

43. (New): The method of claim 39, wherein the challenge-handshake protocol in the step of providing facilitates authentication between the network and the client, which client is a wired client.

44. (New): The method of claim 39, wherein the challenge-handshake protocol in the step of providing is utilized between an authentication server disposed on the network and the client, the authentication server performing an authentication of the client, followed by the client performing an authentication of the network.

45. (New): The method of claim 39, wherein the vendor-specific attribute data is indicative of an encryption key value.

46. (New): The method of claim 45, further comprising extracting the encryption key value by the network access server.

47. (New): The method of claim 46, further comprising sending an encrypted message by the network access server to the client, the encrypted message indicating to the client a key length and key index of the session key.

48. (New): The method of claim 47, further comprising, sending a second message by the network access server to the client, the second encrypted message comprising the key length, key index, and a value of a multicast key.

49. (New): A system of managing access to a network, comprising:

an authentication server disposed on the network to provide an authentication service; and

a network access server disposed on the network in communication with a client seeking access to the network;

wherein the authentication server and the client are adapted to communicate utilizing a challenge-handshake protocol within an Extensible Authentication Protocol for authentication of the client and the authentication server; and

wherein a network session key and a client session key are derived, whereafter successful authentication of both the client to the network and the network to the client, the network session key is used to both create a packet signature and to encrypt a key value of a multicast key that is transmitted from the network access server to the client.

50. (New): The system of claim 49, wherein the challenge-handshake protocol is a CHAP (Challenge-Handshake Authentication Protocol).

51. (New): The system of claim 49, wherein the challenge-handshake protocol is utilized to mutual authenticate the client and the authentication server in response to a single sign-on by a user of the client.

52. (New): The system of claim 49, wherein the challenge-handshake protocol facilitates authentication between the network and the client, which is a wireless client.

53. (New): The system of claim 49, wherein the challenge-handshake protocol facilitates authentication between the network and the client, which client is a wired client.

54. (New): The system of claim 49, wherein the network session key is derived from a username of a user input to the client and transmitted to the authentication server.

55. (New): The system of claim 49, wherein the authentication server performs an authentication of the client, followed by the client performing an authentication of the authentication server.

56. (New): The system of claim 49, wherein after successful mutual authentication between the authentication server and the client, the authentication server passes a session key to the network access server utilizing vendor-specific attribute data.

57. (New): The system of claim 49, wherein the client is a wireless client including a network interface device, the network interface device adapted to host the challenge-handshake protocol utilized for authentication between the wireless client and the network.

58. (New): The system of claim 49, wherein the network access server is a network switch adapted to facilitate communication between the authentication server and the client, which client is a wired client.

59. (New) A system of managing access to a network, comprising:

an authentication server disposed on the network to provide an authentication service; and

a network access server disposed on the network in communication with a client seeking access to the network;

wherein the authentication server and the client are adapted to communicate utilizing a challenge-handshake protocol within an Extensible Authentication Protocol for authentication of the client and the authentication server; and

wherein after successful mutual authentication between the authentication server and the client, the authentication server passes a session key to the network access server utilizing vendor-specific attribute data.

60. (New): The system of claim 59, wherein the challenge-handshake protocol is a CHAP (Challenge-Handshake Authentication Protocol).

61. (New): The system of claim 59, wherein the challenge-handshake protocol is utilized to mutual authenticate the client and the authentication server in response to a single sign-on by a user of the client.

62. (New): The system of claim 59, wherein the challenge-handshake protocol facilitates authentication between the network and the client, which is a wireless client.

63. (New): The system of claim 59, wherein the challenge-handshake protocol facilitates authentication between the network and the client, which client is a wired client.

64. (New): The system of claim 59, wherein a session key is derived for enabling secure communications between the client and the network access server.

65. (New): The system of claim 59, wherein a network session key and a client session key are derived, which client session key is derived independently of the network session key, which both the network session key and the client session key are utilized for enabling secure communications between the client and the network access server.

66. (New): The system of claim 65, wherein the network session key is derived from a username of a user input to the client and transmitted to the authentication server.

67. (New): The system of claim 59, wherein the authentication server performs an authentication of the client, followed by the client performing an authentication of the authentication server.

68. (New): The system of claim 59, wherein a network session key and a client session key are derived, whereafter successful authentication of both the client to the network and the network to the client, the network session key is used to both create a packet signature and to encrypt a key value of a multicast key that is transmitted from the network access server to the client.

69. (New): A system according to claim 59, wherein the vendor-specific attribute data is indicative of an encryption key value.

70 (New): A system according to claim 69, wherein the network access server extracts the encryption key value by the network access server.

71. (New): A system according to claim 70, wherein the network access server responsive to extracting the encryption key value sends an encrypted message to the client, the encrypted message indicating to the client a key length and key index of the session key.

72. (New): A system according to claim 71, wherein the network access server is responsive to extracting the encryption key value to send a second message to the client, the second encrypted message comprising the key length, key index, and a value of a multicast key.

73. (New): The system of claim 59, wherein the client is a wireless client including a network interface device, the network interface device adapted to host the challenge-handshake protocol utilized for authentication between the wireless client and the network.

74. (New): The system of claim 59, wherein the network access server is a network switch adapted to facilitate communication between the authentication server and the client, which client is a wired client.